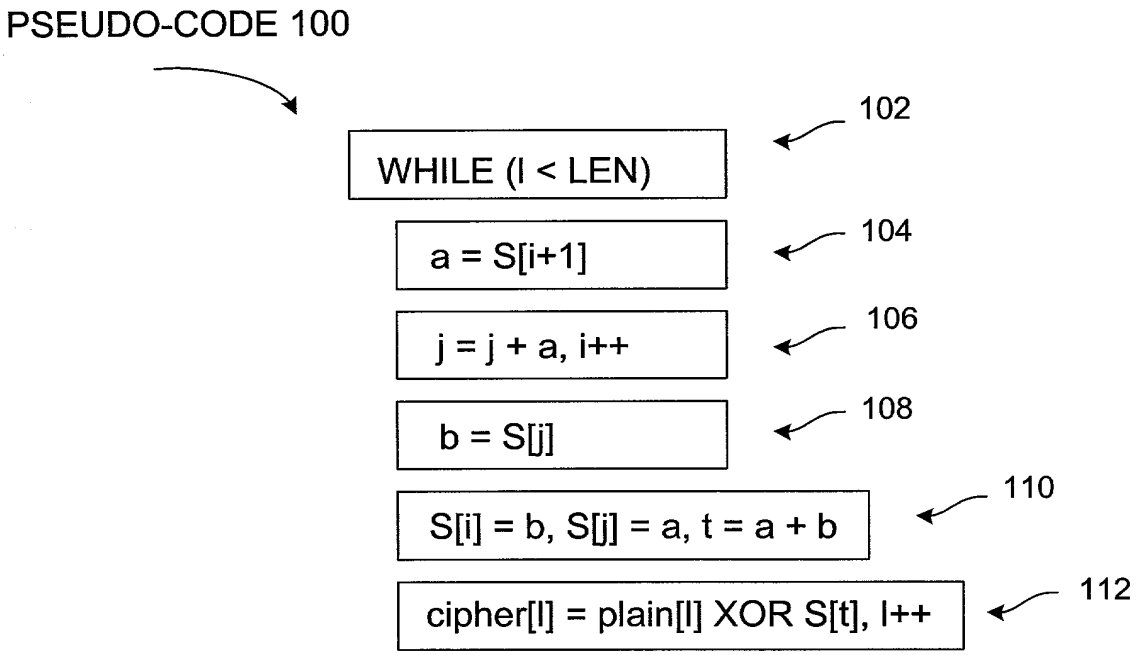

FIG. 1 (PRIOR ART)

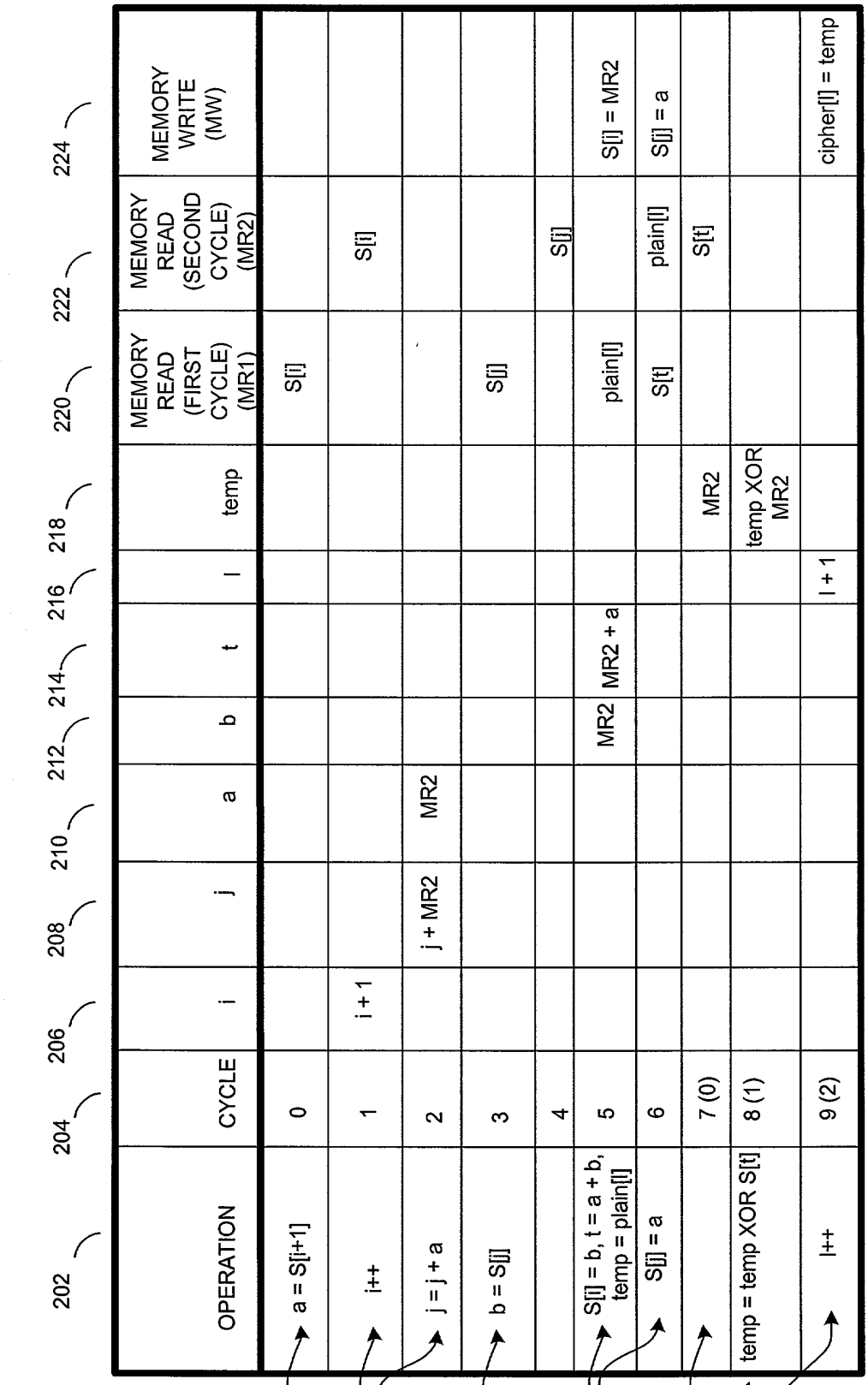

FIG. 2 (PRIOR ART)

200

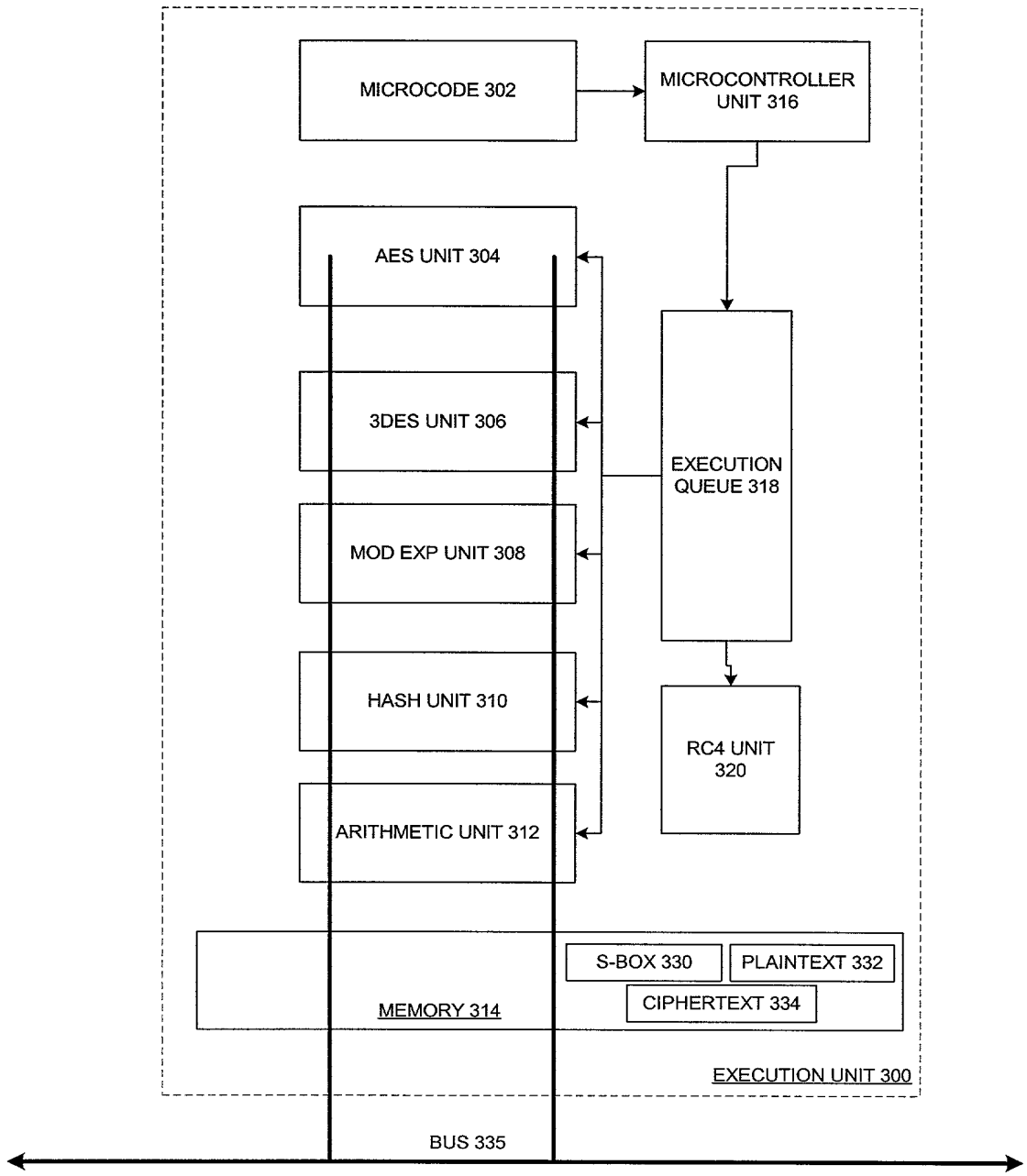
MICROCODE 302
MICROCONTROLLER UNIT 316
AES UNIT 304
3DES UNIT 306
MOD EXP UNIT 308
HASH UNIT 310
ARITHMETIC UNIT 312
EXECUTION QUEUE 318
RC4 UNIT 320
S-BOX 330
PLAINTEXT 332
CIPHERTEXT 334
MEMORY 314
EXECUTION UNIT 300
BUS 335

FIG. 3

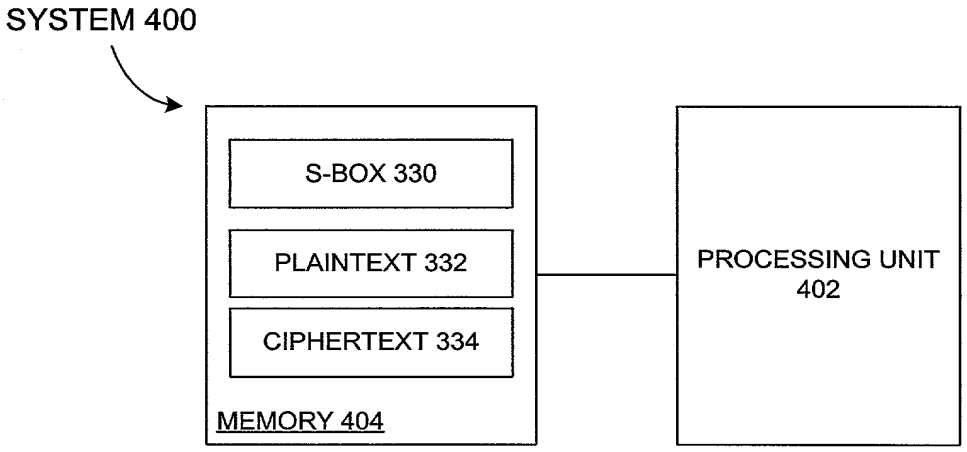

FIG. 4

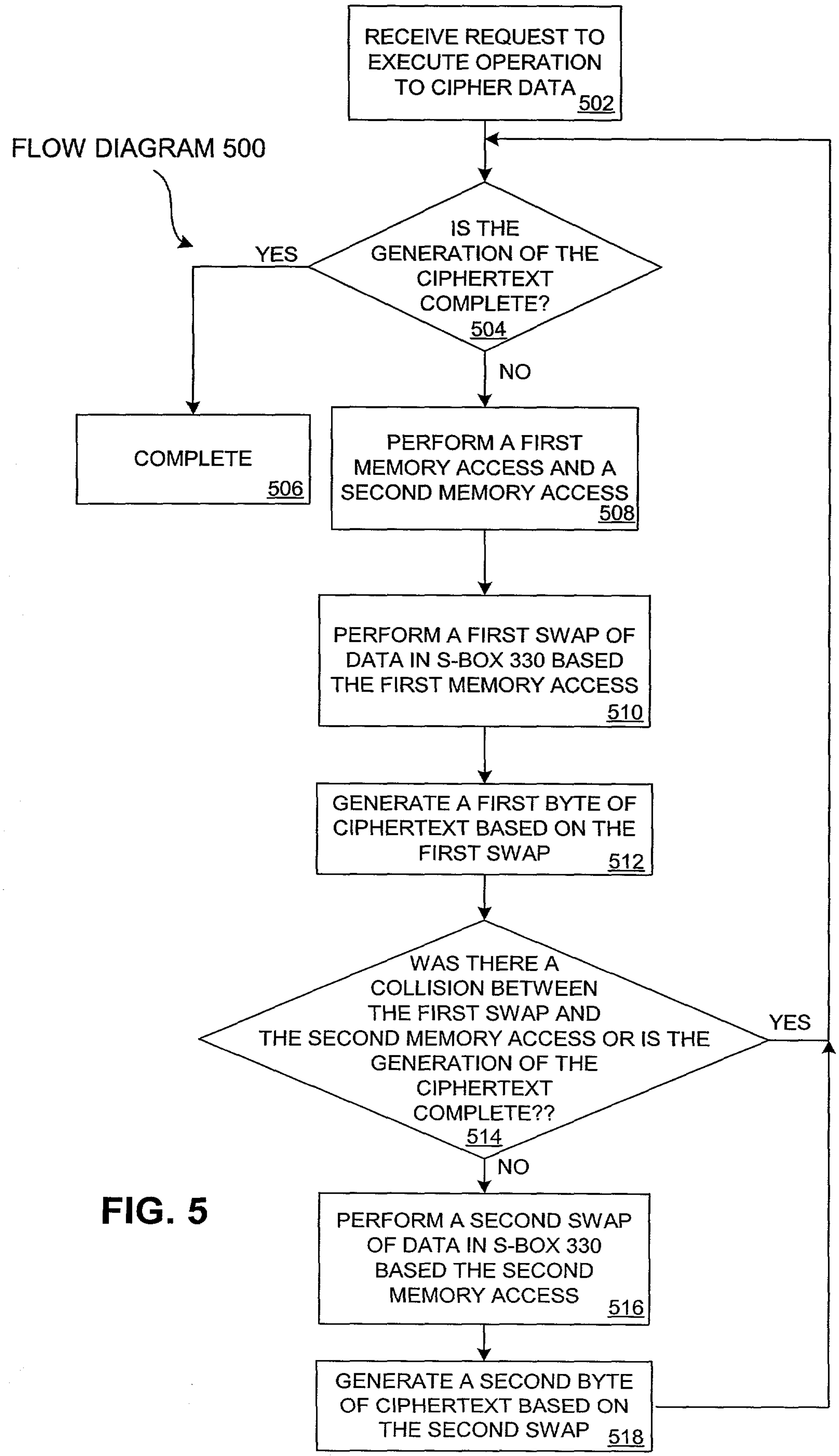

FIG. 5

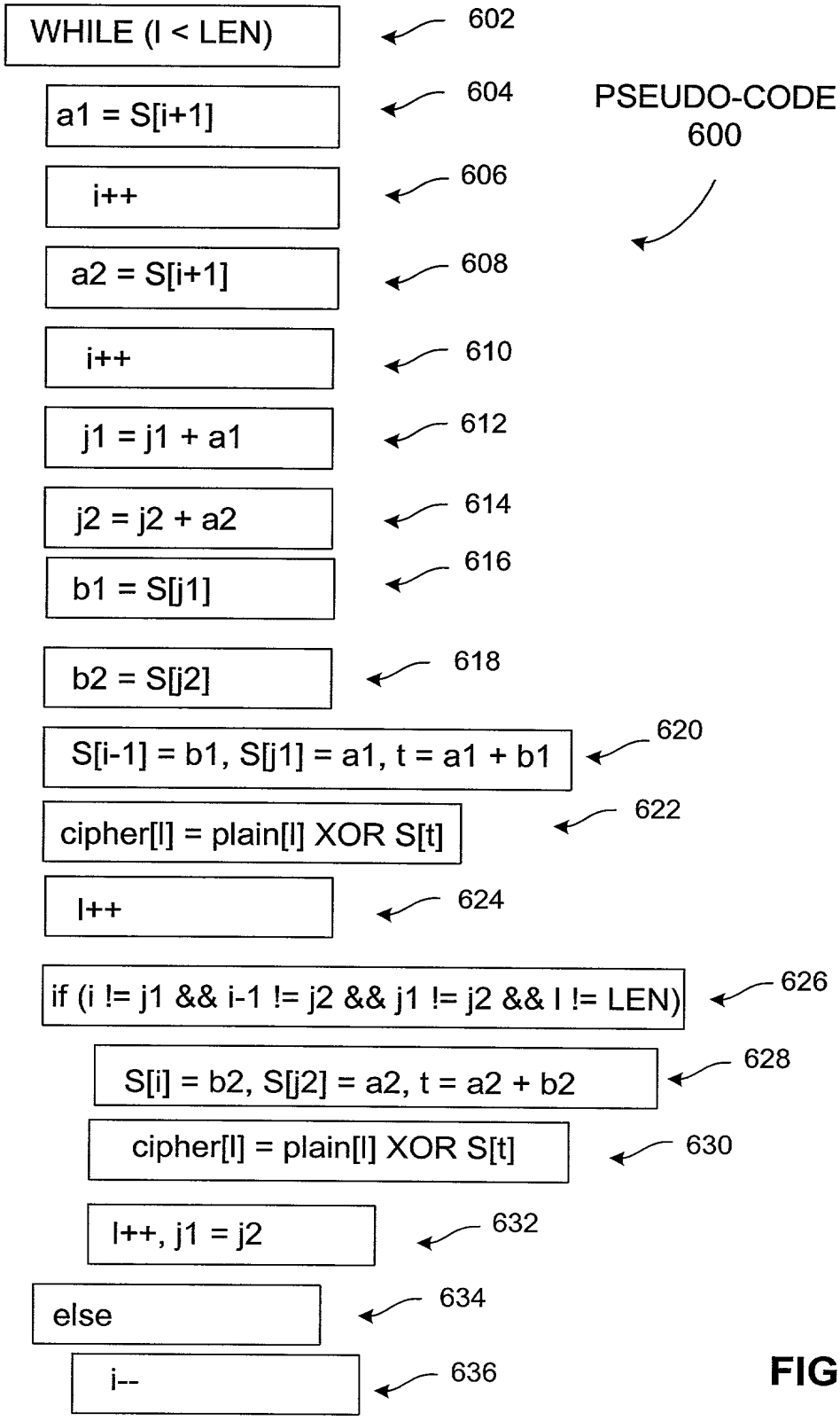

FIG. 6

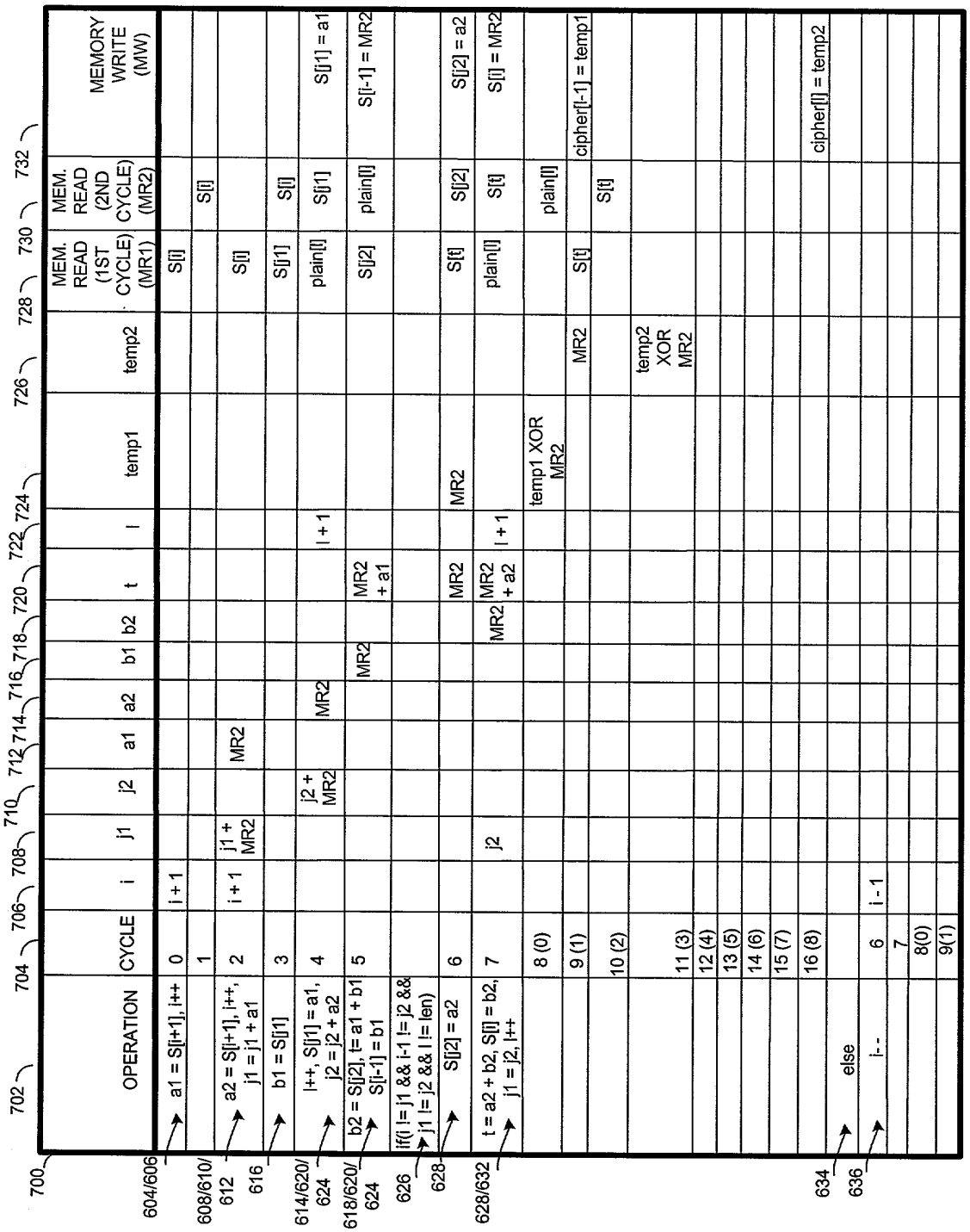
700
702
704
706
708
710
712
714
716
718
720
722
724
726
728
730
732
OPERATION
CYCLE
i
j1
j2
a1
a2
b1
b2
t
l
temp1
temp2
MEM. READ (1ST CYCLE) (MR1)
MEM. READ (2ND CYCLE) (MR2)
MEMORY WRITE (MW)
604/606
608/610/ 612
616
614/620/ 624
618/620/ 624
626
628
628/632
634
636
a1 = S[i+1], i++
a2 = S[i+1], i++, j1 = j1 + a1
b1 = S[j1]
l++, S[j1] = a1, j2 = j2 + a2
b2 = S[j2], t= a1 + b1 S[i-1] = b1
if(i != j1 && i-1 != j2 && j1 != j2 && l != len)
S[j2] = a2
t = a2 + b2, S[l] = b2, j1 = j2, l++
else
i- -
i + 1
j1 + MR2
j2 + MR2
MR2
l + 1
MR2 + a1
MR2 + a2
temp1 XOR MR2
temp2 XOR MR2
S[i]
S[j1]
plain[l]
S[j2]
S[t]
cipher[l-1] = temp1
cipher[l] = temp2
0
1
2
3
4
5
6
7
8 (0)
9 (1)
10 (2)
11 (3)
12 (4)
13 (5)
14 (6)
15 (7)
16 (8)
8(0)
9(1)

FIG. 7

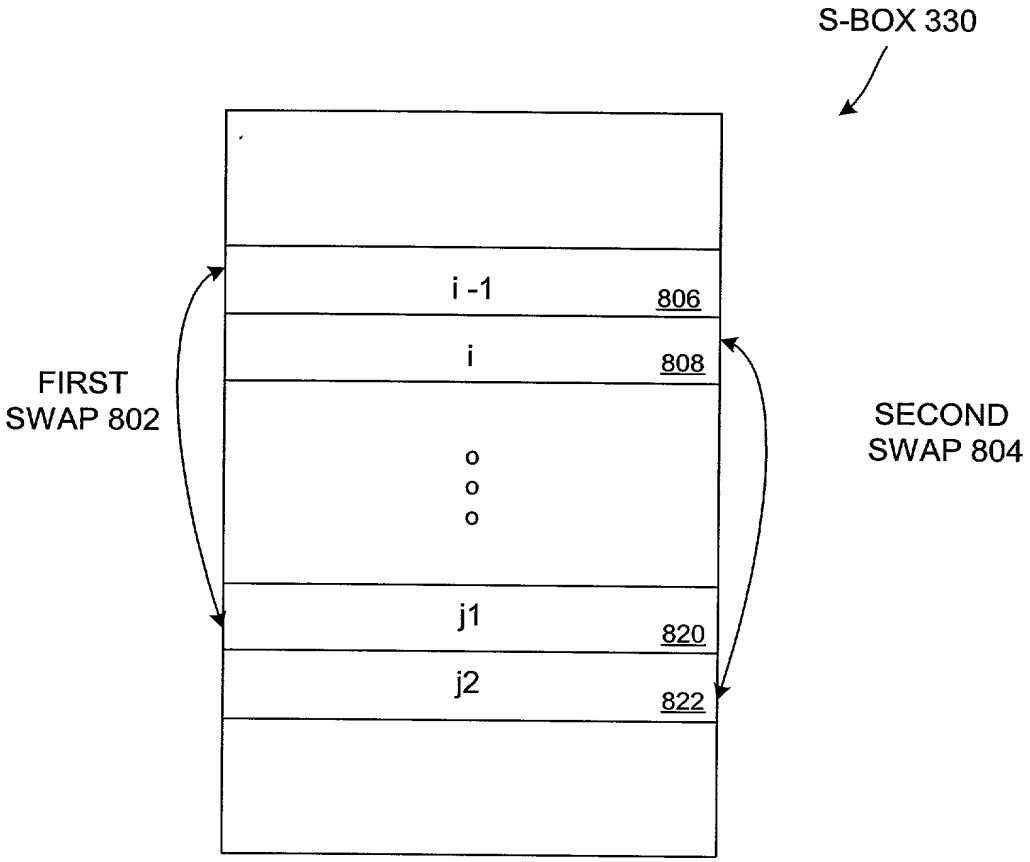
S-BOX 330
i -1
806
i
808
o
o
o
j1
820
j2
822
FIRST
SWAP 802
SECOND
SWAP 804

FIG. 8

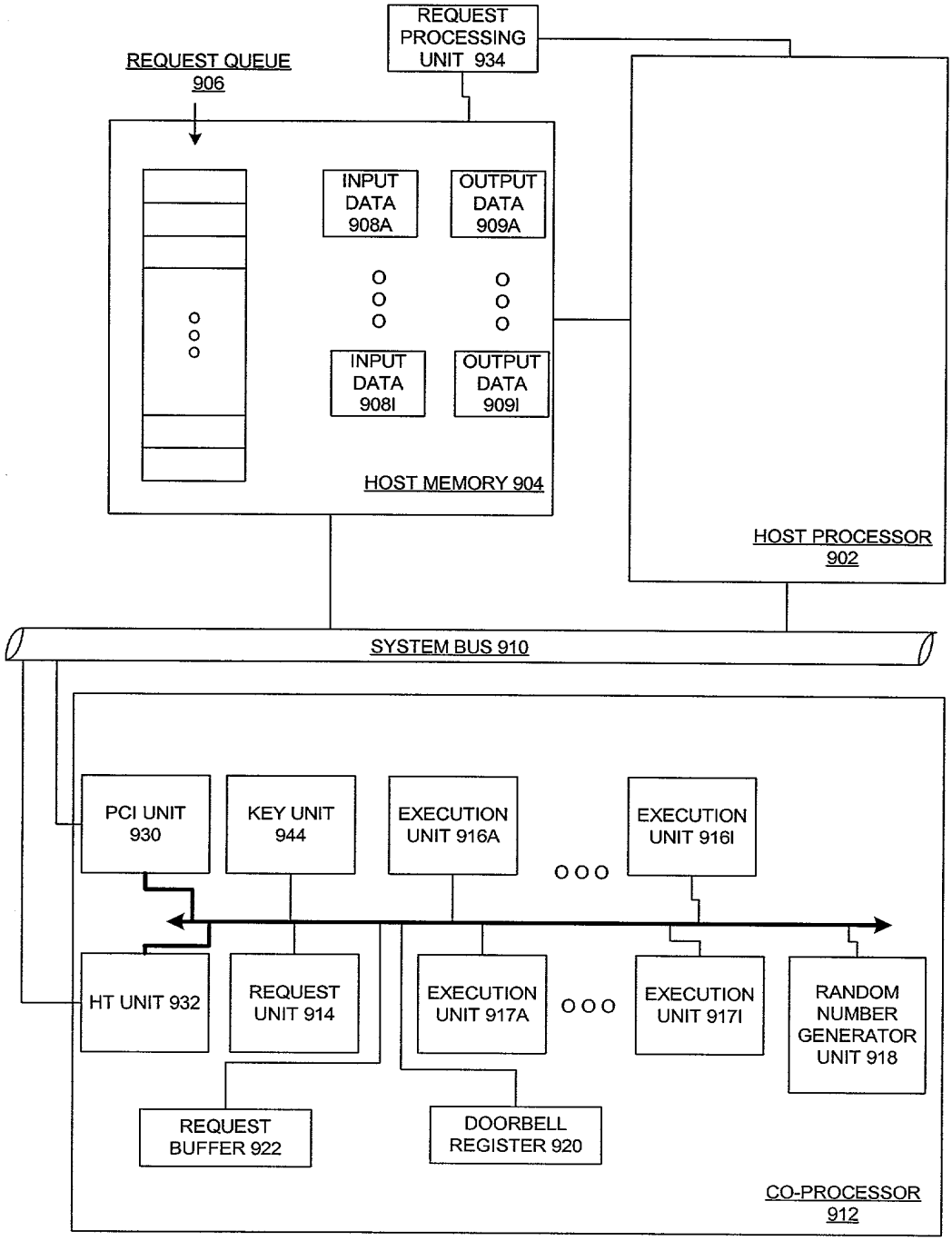
REQUEST PROCESSING UNIT 934
REQUEST QUEUE 906
INPUT DATA 908A
OUTPUT DATA 909A
INPUT DATA 908I
OUTPUT DATA 909I
HOST MEMORY 904
HOST PROCESSOR 902
SYSTEM BUS 910
PCI UNIT 930
KEY UNIT 944
EXECUTION UNIT 916A
EXECUTION UNIT 916I
HT UNIT 932
REQUEST UNIT 914
EXECUTION UNIT 917A
EXECUTION UNIT 917I
RANDOM NUMBER GENERATOR UNIT 918
REQUEST BUFFER 922
DOORBELL REGISTER 920
CO-PROCESSOR 912

FIG. 9